

DOCKET No.

NAI1P055/01.228.01

U.S. PATENT APPLICATION
FOR
SYSTEM, METHOD AND COMPUTER PROGRAM
PRODUCT FOR PRECLUDING WRITES TO
CRITICAL FILES

ASSIGNEE: NETWORKS ASSOCIATES TECHNOLOGY, INC.

SILICON VALLEY IP GROUP
P.O. Box 721120
SAN JOSE, CA 95172

SYSTEM, METHOD AND COMPUTER PROGRAM PRODUCT FOR PRECLUDING WRITES TO CRITICAL FILES

FIELD OF THE INVENTION

5

The present invention relates to network security management, and more particularly to preventing critical files from being overwritten or altered by a virus or other malicious code.

10

BACKGROUND OF THE INVENTION

15

Network security management is becoming a more difficult problem as networks grow in size and become a more integral part of organizational operations. Attacks on networks are growing both due to the intellectual challenge such attacks represent for hackers and due to the increasing payoff for the serious attacker. Furthermore, the attacks are growing beyond the current capability of security management tools to identify and quickly respond to those attacks. As various attack methods are tried and ultimately repulsed, the attackers will attempt new approaches with more subtle attack features. Thus, maintaining network security is on-going, ever changing, and an increasingly complex problem.

20

Computer network attacks can take many forms and any one attack may include many security events of different types. Security events are anomalous network conditions each of which may cause an anti-security effect to a computer network.

25

Security events include stealing confidential or private information; producing network damage through mechanisms such as viruses, worms, or Trojan horses; overwhelming the network's capacities in order to cause denial of service, and so forth.

Network security risk-assessment tools, i.e. "scanners," may be used by a network manager to simulate an attack against computer systems via a remote connection. Such scanners can probe for network weaknesses by simulating certain types of security events that make up an attack. Such tools can also test user passwords for suitability and security. Moreover, scanners can search for known types of security events in the form of malicious programs such as viruses, worms, and Trojan horses.

One common technique for preventing a security event is to preclude the fulfillment of write requests to sensitive files (i.e. executable files, etc.). U.S. Pat. No.: 6,073,239 to Dotan teaches such a system. In particular, a method is disclosed for protecting executable computer programs against infection by a computer virus program. The method prevents writing operations that attempt to modify portions of the program, such as the program's entry point or first instructions. A writing operation that attempts to write data to the program is intercepted and analyzed before the operation is allowed to be processed. The method selects significant data and stores the data, in order to retain information indicative of the program prior to any modification thereof. The method then determines if the writing operation is attempting to modify the significant data, and if it is determined that the writing operation is attempting to modify the data, an alarm is generated and operation is denied. If it is determined that the writing operation is not attempting to modify the data, the writing operation is allowed to continue. Additionally, the program can be restored to its initial state using the stored information and data. The method further uses the stored data indicative of the significant data of the program to restore the program to its initial state and undo all the modifications that the virus may have made to the program.

Unfortunately, such systems have significant limitations in that they are not dynamic, they can not be tailored to a particular system, they do not take into account

the application that makes the write request, and they do not consider the location of the file to be written. There is thus a need for a technique of overcoming these and various other related disadvantages and shortcomings associated with the prior art.

11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
1001
1002
1003
1004
1005
1006
1007
1008
1009
1010
1011
1012
1013
1014
1015
1016
1017
1018
1019
1020
1021
1022
1023
1024
1025
1026
1027
1028
1029
1030
1031
1032
1033
1034
1035
1036
1037
1038
1039
1040
1041
1042
1043
1044
1045
1046
1047
1048
1049
1050
1051
1052
1053
1054
1055
1056
1057
1058
1059
1060
1061
1062
1063
1064
1065
1066
1067
1068
1069
1070
1071
1072
1073
1074
1075
1076
1077
1078
1079
1080
1081
1082
1083
1084
1085
1086
1087
1088
1089
1090
1091
1092
1093
1094
1095
1096
1097
1098
1099
1100
1101
1102
1103
1104
1105
1106
1107
1108
1109
1110
1111
1112
1113
1114
1115
1116
1117
1118
1119
1120
1121
1122
1123
1124
1125
1126
1127
1128
1129
1130
1131
1132
1133
1134
1135
1136
1137
1138
1139
1140
1141
1142
1143
1144
1145
1146
1147
1148
1149
1150
1151
1152
1153
1154
1155
1156
1157
1158
1159
1160
1161
1162
1163
1164
1165
1166
1167
1168
1169
1170
1171
1172
1173
1174
1175
1176
1177
1178
1179
1180
1181
1182
1183
1184
1185
1186
1187
1188
1189
1190
1191
1192
1193
1194
1195
1196
1197
1198
1199
1200
1201
1202
1203
1204
1205
1206
1207
1208
1209
1210
1211
1212
1213
1214
1215
1216
1217
1218
1219
1220
1221
1222
1223
1224
1225
1226
1227
1228
1229
1230
1231
1232
1233
1234
1235
1236
1237
1238
1239
1240
1241
1242
1243
1244
1245
1246
1247
1248
1249
1250
1251
1252
1253
1254
1255
1256
1257
1258
1259
1260
1261
1262
1263
1264
1265
1266
1267
1268
1269
1270
1271
1272
1273
1274
1275
1276
1277
1278
1279
1280
1281
1282
1283
1284
1285
1286
1287
1288
1289
1290
1291
1292
1293
1294
1295
1296
1297
1298
1299
1300
1301
1302
1303
1304
1305
1306
1307
1308
1309
1310
1311
1312
1313
1314
1315
1316
1317
1318
1319
1320
1321
1322
1323
1324
1325
1326
1327
1328
1329
1330
1331
1332
1333
1334
1335
1336
1337
1338
1339
1340
1341
1342
1343
1344
1345
1346
1347
1348
1349
1350
1351
1352
1353
1354
1355
1356
1357
1358
1359
1360
1361
1362
1363
1364
1365
1366
1367
1368
1369
1370
1371
1372
1373
1374
1375
1376
1377
1378
1379
1380
1381
1382
1383
1384
1385
1386
1387
1388
1389
1390
1391
1392
1393
1394
1395
1396
1397
1398
1399
1400
1401
1402
1403
1404
1405
1406
1407
1408
1409
1410
1411
1412
1413
1414
1415
1416
1417
1418
1419
1420
1421
1422
1423
1424
1425
1426
1427
1428
1429
1430
1431
1432
1433
1434
1435
1436
1437
1438
1439
1440
1441
1442
1443
1444
1445
1446
1447
1448
1449
1450
1451
1452
1453
1454
1455
1456
1457
1458
1459
1460
1461
1462
1463
1464
1465
1466
1467
1468
1469
1470
1471
1472
1473
1474
1475
1476
1477
1478
1479
1480
1481
1482
1483
1484
1485
1486
1487
1488
1489
1490
1491
1492
1493
1494
1495
1496
1497
1498
1499
1500
1501
1502
1503
1504
1505
1506
1507
1508
1509
1510
1511
1512
1513
1514
1515
1516
1517
1518
1519
1520
1521
1522
1523
1524
1525
1526
1527
1528
1529
1530
1531
1532
1533
1534
1535
1536
1537
1538
1539
1540
1541
1542
1543
1544
1545
1546
1547
1548
1549
1550
1551
1552
1553
1554
1555
1556
1557
1558
1559
1560
1561
1562
1563
1564
1565
1566
1567
1568
1569
1570
1571
1572
1573
1574
1575
1576
1577
1578
1579
1580
1581
1582
1583
1584
1585
1586
1587
1588
1589
1590
1591
1592
1593
1594
1595
1596
1597
1598
1599
1600
1601
1602
1603
1604
1605
1606
1607
1608
1609
1610
1611
1612
1613
1614
1615
1616
1617
1618
1619
1620
1621
1622
1623
1624
1625
1626
1627
1628
1629
1630
1631
1632
1633
1634
1635
1636
1637
1638
1639
1640
1641
1642
1643
1644
1645
1646
1647
1648
1649
1650
1651
1652
1653
1654
1655
1656
1657
1658
1659
1660
1661
1662
1663
1664
1665
1666
1667
1668
1669
1670
1671
1672
1673
1674
1675
1676
1677
1678
1679
1680
1681
1682
1683
1684
1685
1686
1687
1688
1689
1690
1691
1692
1693
1694
1695
1696
1697
1698
1699
1700
1701
1702
1703
1704
1705
1706
1707
1708
1709
1710
1711
1712
1713
1714
1715
1716
1717
1718
1719
1720
1721
1722
1723
1724
1725
1726
1727
1728
1729
1730
1731
1732
1733
1734
1735
1736
1737
1738
1739
1740
1741
1742
1743
1744
1745
1746
1747
1748
1749
1750
1751
1752
1753
1754
1755
1756
1757
1758
1759
1760
1761
1762
1763
1764
1765
1766
1767
1768
1769
1770
1771
1772
1773
1774
1775
1776
1777
1778
1779
1780
1781
1782
1783
1784
1785
1786
1787
1788
1789
1790
1791
1792
1793
1794
1795
1796
1797
1798
1799
1800
1801
1802
1803
1804
1805
1806
1807
1808
1809
1810
1811
1812
1813
1814
1815
1816
1817
1818
1819
1820
1821
1822
1823
1824
1825
1826
1827
1828
1829
1830
1831
1832
1833
1834
1835
1836
1837
1838
1839
1840
1841
1842
1843
1844
1845
1846
1847
1848
1849
1850
1851
1852
1853
1854
1855
1856
1857
1858
1859
1860
1861
1862
1863
1864
1865
1866
1867
1868
1869
1870
1871
1872
1873
1874
1875
1876
1877
1878
1879
1880
1881
1882
1883
1884
1885
1886
1887
1888
1889
1890
1891
1892
1893
1894
1895
1896
1897
1898
1899
1900
1901
1902
1903
1904
1905
1906
1907
1908
1909
1910
1911
1912
1913
1914
1915
1916
1917
1918
1919
1920
1921
1922
1923
1924
1925
1926
1927
1928
1929
1930
1931
1932
1933
1934
1935
1936
1937
1938
1939
1940
1941
1942
1943
1944
1945
1946
1947
1948
1949
1950
1951
1952
1953
1954
1955
1956
1957
1958
1959
1960
1961
1962
1963
1964
1965
1966
1967
1968
1969
1970
1971
1972
1973
1974
1975
1976
1977
1978
1979
1980
1981
1982
1983
1984
1985
1986
1987
1988
1989
1990
1991
1992
1993
1994
1995
1996
1997
1998
1999
2000
2001
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
2031
2032
2033
2034
2035
2036
2037
2038
2039
2040
2041
2042
2043
2044
2045
2046
2047
2048
2049
2050
2051
2052
2053
2054
2055
2056
2057
2058
2059
2060
2061
2062
2063
2064
2065
2066
2067
2068
2069
2070
2071
2072
2073
2074
2075
2076
2077
2078
2079
2080
2081
2082
2083
2084
2085
2086
2087
2088
2089
2090
2091
2092
2093
2094
2095
2096
2097
2098
2099
2100
2101
2102
2103
2104
2105
2106
2107
2108
2109
2110
2111
2112
2113
2114
2115
2116
2117
2118
2119
2120
2121
2122
2123
2124
2125
2126
2127
2128
2129
2130
2131
2132
2133
2134
2135
2136
2137
2138
2139
2140
2141
2142
2143
2144
2145
2146
2147
2148
2149
2150
2151
2152
2153
2154
2155
2156
2157
2158
2159
2160
2161
2162
2163
2164
2165
2166
2167
2168
2169
2170
2171
2172
2173
2174
2175
2176
2177
2178
2179
2180
2181
2182
2183
2184
2185
2186
2187
2188
2189
2190
2191
2192
2193
2194
2195
2196
2197
2198
2199
2200
2201
2202
2203
2204
2205
2206
2207
2208
2209
2210
2211
2212
2213
2214
2215
2216
2217
2218
2219
2220
2221
2222
2223
2224
2225
2226
2227
2228
2229
2230
22

DISCLOSURE OF THE INVENTION

A system, method and computer program product are provided for preventing writes to critical files. Initially, factors associated with a computer are identified. Then,
5 requests to write to files on the computer are monitored. The writes to the files on the computer are conditionally prevented based on the factors to prevent virus proliferation. In use, the factors are altered based on the monitoring of the requests.

In one embodiment, the factors are selected from the group consisting of critical
10 files, critical file locations, and trusted applications. Such factors may be user configurable. Further, the factors may be identified in a registry.

In another embodiment, the factors may include critical files associated with an operating system of the computer. In addition, the factors may include critical file
15 locations associated with an operating system of the computer. Such critical file locations may include folders. Still yet, the factors may include trusted applications that initiate the requests.

In still another embodiment, the factors may be updated based on a user request.
20 Further, the factors may be updated from a remote location via a network. Also, the factors may be updated based at least in part on the manner and nature of the write requests. By these updates, the present embodiment may “learn” about the system, and better prevent writes to critical files.

25 In use, writes to the files on the computer may also be conditionally prevented based on a user confirmation. Still yet, the factors may be updated based on the user confirmation.

BRIEF DESCRIPTION OF THE DRAWINGS

Figure 1 illustrates a network architecture, in accordance with one embodiment.

5

Figure 2 shows a representative hardware environment that may be associated with the data servers and computers of Figure 1, in accordance with one embodiment.

Figure 3 illustrates a method for generating a plurality of factors on which critical file write-protection may be based.

10

Figure 4 illustrates an exemplary data structure that results from the method of Figure 3.

Figure 5 is a flowchart showing a method for conditionally preventing writes to files, in accordance with one embodiment.

15

DESCRIPTION OF THE PREFERRED EMBODIMENTS

Figure 1 illustrates a network architecture 100, in accordance with one embodiment. As shown, a plurality of networks 102 is provided. In the context of the present network architecture 100, the networks 102 may each take any form including, but not limited to a local area network (LAN), a wide area network (WAN) such as the Internet, etc.

Coupled to the networks 102 are data servers 104 which are capable of communicating over the networks 102. Also coupled to the networks 102 and the data servers 104 is a plurality of end user computers 106. In the context of the present description, such end user computers 106 may include a web server, desktop computer, lap-top computer, hand-held computer, printer or any other type of hardware/software.

In order to facilitate communication among the networks 102, at least one gateway 108 is coupled therebetween. It should be noted that each of the foregoing network devices as well as any other unillustrated devices may be interconnected by way of a plurality of network segments.

While shown attached to the gateway 108, any of the foregoing components and/or segments may be equipped with a scanner 120 including anti-virus scanning software. Such scanner 120 may be equipped to probe for network weaknesses by simulating certain types of security events that make up an attack. Such scanner 120 may also test user passwords for suitability and security. Moreover, the scanner 120 may also search for known types of security events in the form of malicious programs such as viruses, worms, and Trojan horses. Still yet, [0]the scanner 120 may be adapted for content filtering to enforce an organization's operational policies [i.e. detecting

harassing or pornographic content, junk e-mails, misinformation (virus hoaxes), etc.].
Of course, the scanner 120 may take any other sort of security measures.

Instead of or in addition to the foregoing capabilities, the scanner 120 may
5 operate to prevent critical files from being written. Initially, factors associated with a
computer are identified. Then, requests to write to files on the computer are monitored.
The writes to the files on the computer are conditionally prevented based on the factors
to prevent virus proliferation. In use, such factors are altered based on the monitoring of
the requests.

10 By this design, writes to critical files are prevented based on certain factors.
Moreover, such factors are updated during and based on use of the system. More
information regarding an exemplary application of such technique will be set forth
hereinafter in greater detail.

15 Figure 2 shows a representative hardware environment that may be associated
with the data servers 104 and/or end user computers 106 of Figure 1, in accordance with
one embodiment. Such figure illustrates a typical hardware configuration of a
workstation in accordance with a preferred embodiment having a central processing unit
20 210, such as a microprocessor, and a number of other units interconnected via a system
bus 212.

The workstation shown in Figure 2 includes a Random Access Memory (RAM)
214, Read Only Memory (ROM) 216, an I/O adapter 218 for connecting peripheral
25 devices such as disk storage units 220 to the bus 212, a user interface adapter 222 for
connecting a keyboard 224, a mouse 226, a speaker 228, a microphone 232, and/or other
user interface devices such as a touch screen (not shown) to the bus 212, communication
adapter 234 for connecting the workstation to a communication network 235 (e.g., a

data processing network) and a display adapter **236** for connecting the bus **212** to a display device **238**.

The workstation may have resident thereon an operating system such as the Microsoft Windows NT or Windows/95 Operating System (OS), the IBM OS/2 operating system, the MAC OS, or UNIX operating system. It will be appreciated that a preferred embodiment may also be implemented on platforms and operating systems other than those mentioned. A preferred embodiment may be written using JAVA, C, and/or C++ language, or other programming languages, along with an object oriented programming methodology. Object oriented programming (OOP) has become increasingly used to develop complex applications.

Figure **3** illustrates a method **300** for generating a plurality of factors on which critical file write-protection may be based. In one embodiment, the present method **300** may be used in the context of a scanner like that mentioned hereinabove during reference to Figure **1**. Of course, the present techniques may be utilized in any desired context.

Initially, an operating system associated with a system to be monitored is identified. Note operation **301**. It should be noted that each operating system may be identified as a particular brand, type, version, etc. In addition to the particular operating system, certain applications may also be identified along with any other particular feature or aspect of the system.

Once identified, various critical files are looked up based on the identified operating system and any other of the foregoing characteristics. See operation **302**. In one embodiment, this may be accomplished by maintaining a local or remote default list of critical files for each known operating system, application, etc. As will soon become

apparent, such default list of critical files may be updated during use of the system as the scanner “learns” about the use thereof.

In addition to using the default list, critical file entries may also be identified from a registry in operation 304. A registry typically includes information such as what hardware is attached to the system, what system options have been selected, how computer memory is set up, and what application programs are to be present when the operating system is started.

It should be noted that certain files may be deemed critical files based on an extension thereof. For example, executable files with a *.EXE extension may be considered critical by default. In a similar manner, files with a *.DLL may also be deemed critical.

In addition to critical files, critical file locations may be identified in operation 306. Such critical file locations may each include a particular directory, folder or other portion of memory where critical files are stored. For example, an operating system directory or folder may be considered a critical file location, while a temporary file location would not. Such critical file locations may be identified in a manner similar or different from that associated with the critical file identification process.

Still another factor to be identified includes trusted applications that will be accessing the various files and file locations. See operation 308. Similar to the critical file locations, the trusted applications may be identified in a manner similar or different from that associated with the critical file identification process. In the context of the present description, the applications may be identified based on a type, version, location, etc. thereof. For example, any local application not located remote from a system may be considered trusted.

It should be noted that the various factors may be selected and updated in any desired manner. For example, if it is determined that a user wishes to manually contribute to the configuration process in decision **310**, any one of the foregoing factors may be added, removed, or otherwise altered per the desires of the user. See operation **312**. This may be accomplished utilizing any desired interface. Further, if it is determined an administrator or other remote agent wishes to manually or automatically contribute to the configuration process in decision **314**, any one of the foregoing factors may be added, removed, or otherwise altered remotely via a network. See operation **316**.

It should be noted that the foregoing factors may influence a decision to preclude the fulfillment of a write request in order to prevent the proliferation of a virus or any damaging consequences associated therewith.

Figure **4** illustrates an exemplary data structure **400** that results from the method **300** of Figure **3**. Of course, the various factors may be organized, stored, etc. in any desired manner. As shown in Figure **4**, the data structure **400** includes a plurality of critical files **406**, a plurality of critical file locations **408**, and trusted applications **410**.

Figure **5** is a flowchart showing a method **500** for conditionally preventing writes to files, in accordance with one embodiment. Provided with a list of factors such as those set forth during reference to Figure **4**, the present method **500** is capable of conditionally preventing writes to files based on the factors. Further, the present method **500** is adapted for updating the factors during the course of use of the system, in a manner that will soon become apparent.

The present method **500** is initiated upon the receipt of a write request in operation **501**. Such write request may be initiated in any desired manner. For example, the write request may be received from a user, an application, from a remote computer, etc. Further, the write request may identify a file to be written.

5

It is then determined in decision **502** whether the location of the file to be written is in a critical file location. This may be accomplished by simply comparing the file location with a data structure like that shown in Figure 4. If not, the write may be permitted in operation **512**. As an option, additional security features may be initiated before permitting such write.

10

If, however, it is determined in decision **502** that the location of the file to be written is in a critical file location, it is then determined whether the application initiating such write request is trusted. See decision **504**. Again, this may be accomplished by simply comparing the application with a data structure like that shown in Figure 4. If the application is not trusted, the user is alerted in operation **506**. This may be accomplished in any desired manner. For example, a visual notification may be displayed on the computer or at any remote location.

15

Next, it is determined in decision **508** whether a user will permit the write request from the untrusted application. This may be accomplished by simply prompting the user to OK the write utilizing a pop-up window or the like. If the user does not OK the write, the write and any access to the file may be denied in operation **510**, after which the method **500** is terminated until another write request is received.

20

25

If, however, the user does OK the write, it is then determined whether the user is permitting the fulfillment of the present write request from the untrusted application, or all future write requests from the untrusted application. See decision **512**. Again, this

may be accomplished by simply prompting the user to decide using a pop-up window or the like. If the user wishes to permit all future write requests from the untrusted application in decision **512**, the application may be added as a trusted application in a data structure such as that of Figure 4. In any case, the write is permitted in operation **512**.

Returning again to decision **504**, if it is determined that the application initiating such write request is trusted, it is then determined whether the file is critical. See decision **514**. Similar to before, this may be accomplished by simply comparing the application with a data structure like that shown in Figure 4. If the file is critical, the user is alerted to this fact in operation **516**. This may be accomplished in any desired manner. For example, a visual notification may be displayed on the computer or at any remote location.

Next, it is determined in decision **518** whether a user will permit the write to the critical file. This may be accomplished by simply prompting the user to OK the write utilizing a pop-up window or the like. If the user does not OK the write, the write and any access to the file may be denied in operation **520**, after which the method **500** is terminated until another write request is received.

If, however, the user does OK the write, it is then determined whether the user is permitting the fulfillment of the present write request to the critical file, or all future write requests to the critical file. See decision **522**. Again, this may be accomplished by simply prompting the user to decide using a pop-up window or the like. If the user wishes to permit all future writes to the critical file in decision **522**, the crucial file may be removed as a critical file in a data structure such as that of Figure 4. In any case, the write is permitted in operation **512**.

While various embodiments have been described above, it should be understood that they have been presented by way of example only, and not limitation. For example, any of the network elements may employ any of the desired functionality set forth hereinabove. Thus, the breadth and scope of a preferred embodiment should not be

5 limited by any of the above-described exemplary embodiments, but should be defined only in accordance with the following claims and their equivalents.

TELECOM